AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

FILED
RICHARD W. NAGEL
CLERK OF COURT
2022 APR 22 PM 3:15
U.S. DISTRICT COURT
SOUTHERN DIST. OHIO
WESTERN DIV DAYTON

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with the Google account sentai.sensei@gmail.com that is stored at premises controlled by Google LLC

Case No. 3:22 mj 133

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A-1

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B-1

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
SEE ATTACHMENT C-1	

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

☑ Continued on the attached sheet.

☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _______ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Andrea R. Kinzig
Applicant's signature

Andrea R. Kinzig, FBI Special Agent
Printed name and title

Attested to by the applicant in my presence

Date: 4/22/2022

Judge's signature

City and state: Dayton, OH

Michael J. Newman, U.S. District Court Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a) and 2252A). I have received training in the area of child pornography and child exploitation and have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.

2. Along with other agents, officers, and investigators of the FBI, I am currently involved in an investigation of child pornography offenses committed by GEORGE GIBBS III (hereinafter referred to as "GIBBS"). This Affidavit is submitted in support of Applications for search warrants for the following:

   a. Information associated with the Google account **sentai.sensei@gmail.com** that is stored at premises controlled by Google LLC (as more fully described in Attachment A-1); and

   b. Information associated with the Kik account with the user name of **Sentai_Sensei** and the Kik group account with the group name of **#underfifteen** that is stored at premises controlled by MediaLab.ai Inc. (as more fully described in Attachment A-2).

3. The purpose of the Applications is to search for and seize evidence of suspected violations of the following:

   a. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) and 2252A(a)(5)(B) and (b)(2), which make it a crime to possess child pornography; and

   b. 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1), which make it a crime to distribute and receive child pornography through interstate commerce.

4. The items to be searched for and seized are described more particularly in Attachments B-1 and B-2 hereto and are incorporated by reference.

5. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents, officers, and investigators involved in the

investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.

6. This Affidavit is intended to show that there is sufficient probable cause to support the searches of the above noted accounts (as defined in Attachments A-1 and A-2). It does not contain every fact known to the investigation.

7. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; and/or property designed for use, intended for use, or used in committing a crime of violations of federal law, including 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2), 2252A(a)(5)(B) and (b)(2), 2252(a)(2) and (b)(1), and 2252A(a)(2) and (b)(1), are present within the information associated with the above noted accounts (as described in Attachments A-1 and A-2).

JURISDICTION

8. This court has jurisdiction to issue the requested warrants because it is "a court of competent jurisdiction" 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States" that "has jurisdiction over the offense being investigated" 18 U.S.C. § 2711(3)(A)(i).

PERTINENT FEDERAL CRIMINAL STATUTES

9. 18 U.S.C. §§ 2252(a)(2) and (b)(1) state that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

10. 18 U.S.C. §§ 2252A(a)(2) and (b)(1) state that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

11. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) state that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

12. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) state that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

BACKGROUND INFORMATION

Definitions

13. The following definitions apply to this Affidavit and Attachments B-1 and B-2 to this Affidavit:

a. "**Child Pornography**" includes the definition in Title 18 U.S.C. § 2256(8): any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

b. "**Visual depictions**" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).

c. "**Minor**" means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).

d. "**Sexually explicit conduct**" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic

abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. § 2256(2)).

e. **"Child erotica"**, as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

f. **"Internet Service Providers"** or **"ISPs"** are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

g. An **"Internet Protocol address"**, also referred to as an **"IP address"**, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as "octets," ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).

h. **"Hyperlink"** (often referred to simply as a "link") refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. "resource") to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.

i. "**Website**" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

j. "**Uniform Resource Locator**" or "**Universal Resource Locator**" or "**URL**" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

k. "**Social Media**" is a term to refer to websites and other Internet-based applications that are designed to allow people to share content quickly, efficiently, and on a real-time basis. Many social media applications allow users to create account profiles that display users' account names and other personal information, as well as to exchange messages with others. Numerous forms of social media are presently available on the Internet.

<u>Google Services</u>

14. Google LLC ("Google") is a multi-national corporation with its headquarters located in Mountain View, California. Google offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

15. In addition, Google offers an operating system ("OS") for mobile devices (including cellular phones) known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

16. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google

Account. However, users can also sign up for Google accounts with third-party email addresses.

17. Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below. Google's services include but are not limited to the following:

a. Gmail: Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses ("recovery," "secondary," "forwarding," or "alternate" email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

b. Contacts: Google provides address books for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Google Contacts can store up to 25,000 contacts. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their Android mobile phone or device address book with their account so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them. Contacts can be accessed from the same browser window as other Google products like Gmail and Calendar.

c. Calendar: Google provides an appointment book for Google Accounts through Google Calendar, which can be accessed through a browser or mobile application. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device calendar so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the user deletes them. Calendar can be accessed from the same browser window as other Google products like Gmail and Calendar.

d. Messaging: Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to

send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the messages, though other factors may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.

e. Google Drive: Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me". Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

f. Google Keep: Google Keep is a cloud-based notetaking service that lets users take notes and share them with other Google users to view, edit, or comment. Google Keep notes are stored indefinitely, unless the user deletes them. Android device users can also use Google Drive to backup certain data from their device. Android backups on Google Drive may include mobile application data, device settings, file downloads, and SMS messages. If a user subscribes to Google's cloud storage service, Google One, they can opt to backup all the data from their device to Google Drive.

g. Google Photos: Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.

h. Google Maps: Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-by turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location

Sharing feature. And users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.

i. Location History: Google collects and retains data about the location at which Google Account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Precision location data is typically stored by Google in an account's Location History and is assigned a latitude-longitude coordinate with a meter radius margin of error. Inferential data is stored with an account's Web & App Activity. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen months. Accounts created after June 2020 auto-delete Location History after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

j. Chrome and My Activity: Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account in a record called My Activity.

k. Android Backup: Android device users can use Google Drive to backup certain data from their device. Android backups on Google Drive may include mobile application data, call history, contacts, device settings, or SMS messages. Users can also opt-in through Google One to back up photos, videos, and multimedia sent using Messages

18. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through

their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

19. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

20. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

21. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

22. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

23. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal

activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation.

24. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

25. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

26. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

27. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

Kik Messenger Application

28. Kik is a cross-platform instant messenger application available on smartphones. The application allows users to exchange text-based conversations with one another and to share media such as photos, YouTube videos, and other content.

29. The Kik messenger application is administered by MediaLab.ai Inc., a company based in Santa Monica, California. The application can be downloaded free of charge from the Internet. It requires a smartphone with either a data plan or access to a Wi-Fi network to use.

30. Unlike many other smartphone instant messenger applications that are based on a user's telephone number, Kik uses usernames to identify its users. Each user selects and is assigned a unique user name for use on Kik's platform. Each user also creates a user profile, which includes a first and last name and an email address. MediaLab.ai Inc. does not verify this information, and as such, users can provide inaccurate information.

31. MediaLab.ai Inc. maintains users' profile information and collects IP addresses utilized by users to access the account and transmit messages. In some circumstances, MediaLab.ai Inc. also collects users' dates of birth as well as other information about how users have used the messenger application. MediaLab.ai Inc. will only release current information to law enforcement pursuant to service of proper legal service (typically profile information and IP addresses for the past thirty days, or the most recent thirty days if the account has not been recently used). MediaLab.ai Inc. does not store or maintain chat message content.

32. Based on my training and experience, I know that individuals involved in child pornography offenses often utilize the Kik messenger application to trade child pornography files and to communicate with other offenders and victims. In my experience, a number of child pornography offenders believe that the Kik messenger application is a secure means of trading child pornography.

33. According to its current Law Enforcement Guide, MediaLab.ai Inc. maintains on its servers the following account information for its users:

a. Basic subscriber data, including the current first and last names and email addresses, links to the most current profile pictures or background photographs, device related information, account creation dates and Kik versions, birthdays and email addresses used to register the accounts, and users' location information (including IP addresses).

b. Transactional chat logs, which are logs of all the messages that users have sent and received, including senders' usernames, receivers' usernames, receivers' group JID's[1], timestamps, IP addresses of the senders, and word counts;

c. Chat platform logs, which are logs of all the media files that users have sent and received, including senders' usernames, receivers' usernames, receivers' JID's, timestamps, IP addresses of the senders, media types, and Content ID's;

d. Photographs and/or videos sent or received by the users for the last 30 days;

1 JID's are unique internal identification numbers associated with users and group chats. They are randomly generated by Kik's internal system.

e. Roster logs, which are logs of usernames added and blocked by the subject user (including timestamps);

f. Abuse reports, which are transcripts of reported chat histories against the subject user, including the senders' usernames, receivers' usernames, timestamps, actual messages, and content ID's;

g. Email events, which are logs of all the emails that have been associated with a username; and

h. Registration IP's, which are the IP addresses associated to the usernames when the accounts were registered (including the timestamps).

34. Also according to its current Law Enforcement Guide, MediaLab.ai Inc. maintains on its servers the following account information for its groups:

a. Group information logs, which provide current information about the group, including the group JID, group name(s), group type, and the status of the group;

b. Group create logs, which provide details about who created the group and at what time;

c. Group join logs, which provide a record of the users who have joined the group, including timestamps and the method that was used to join a group;

d. Group leave logs, which provide a record of the users who have left the group, including timestamps and the method that was used to leave the group;

e. Group transactional chat logs, which provide a log of all the messages that a group has received, including sender username, timestamps, IP of the sender, receiver username(s), and word count;

f. Group chat platform logs, which provide a log of all the media files that a group has received, including sender username, timestamps, IPs of the sender, receiver username(s), media type, and content ID;

g. Photographs and/or videos received by the group;

h. Group abuse reports, which are transcripts of reported chat history against the subject group, including sender username, receiver username, timestamps, actual message, and content ID's.

Virtual Private Networks

35. A Virtual Private Network, commonly known as a VPN, provides programming that creates a safe and encrypted connection over a less secure network, such as the public Internet. A VPN works by using a shared public infrastructure while maintaining privacy through security procedures and tunneling protocols.

36. A VPN extends a private network across a public network, and it enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running on a computing device (such as a laptop, desktop computer, or smartphone) across a VPN may benefit from the functionality, security, and management of the private network. Encryption is a common though not inherent part of a VPN connection. A number of Electronic Service Providers offer VPN's to customers worldwide.

37. VPN's assign users different IP addresses and run users' data through different servers. As a result, it is very difficult (if not often virtually impossible) for third parties to track the users' identities and browsing activities. Based on my training and experience, I know that individuals involved in child pornography offenses and other illegal activities sometimes use VPN's to conceal their activities from law enforcement officers.

Cloud Storage

38. Cloud computing has become an increasingly popular way for both individuals and businesses to store and maintain data. Cloud computing is the delivery of computing services – including servers, storage, databases, networking, software, analytics, and intelligence – over the Internet (the "cloud"). Cloud computing utilizes computer resources delivered as a service over a network (typically the Internet). Resources are distributed across a variety of remote data centers in different locations.

39. Mega is a cloud storage and file hosting service offered by Mega Limited (Ltd.), an Auckland, New Zealand-based company. Mega is known for its security feature where all files are end-to-end encrypted locally before they are uploaded. This encryption prevents anyone from accessing the files without knowledge of the pass key.

40. Mega provide its users with the ability to share files or folders with others. One means of sharing files or folders is by creating a "sharing link". A sharing link creates a URL to store the file(s) or folder(s) so that others can access, view, and/or download them. These sharing links can be sent to others via email, Facebook, Twitter, instant message, or other means. Users can limit who can access their sharing links by setting passwords and/or expiration dates for the links.

NCMEC and CyberTipline Reports

41. The National Center for Missing and Exploited Children (commonly known as "NCMEC") was founded in 1984 to serve as a clearinghouse on issues related to missing and sexually exploited children. It is currently authorized by Congress to perform 19 programs and services to assist law enforcement, families, and professions find missing children, reduce child sexual exploitation, and prevent child victimization.

42. As part of its functions, NCMEC administers the CyberTipline. The CyberTipline receives leads and tips from the public and Electronic Service Providers regarding suspected crimes of sexual exploitation committed against children. Electronic Service Providers are required by law to report apparent child pornography to law enforcement via the CyberTipline. Analysts review these tips and refer them to the appropriate federal, state, and local law enforcement authorities. Many states utilize Internet Crimes Against Children (ICAC) task forces to serve as the intake organizations for the CyberTipline reports. These ICAC's review the CyberTipline reports received from NCMEC and assign them to the applicable law enforcement agencies. In Ohio, the ICAC in Cuyahoga County serves as this intake organization.

FACTS SUPPORTING PROBABLE CAUSE

Records from MediaLab.ai Inc.

43. On or around December 4, 2020, MediaLab.ai Inc. filed a report to NCMEC's CyberTipline regarding suspected child pornography and/or child exploitation files that were located in a Kik account utilizing the user name of kuro_shinigami444. NCMEC forwarded MediaLab.ai Inc.'s CyberTipline report, along with the suspected child pornography or child exploitation files, to the FBI for further investigation. I obtained and reviewed the CyberTipline Report and the accompanying files as part of the investigation.

44. On or around January 12, 2021, MediaLab.ai Inc. was served with an administrative subpoena requesting subscriber information for the kuru_shinigami444 Kik account as well as the log of IP addresses that were utilized to access the account. On or around July 28, 2021, MedaiLab.ai Inc. was served with a federal search warrant requesting information associated with the kuro_shinigami444 Kik account. Although MediaLab.ai Inc. does not maintain the contents of messages for its account users, it does maintain various log files regarding the activity occurring in the accounts – such as transactional chat logs (which are logs of all messages that users have sent and received) and chat platform logs (which are logs of media files that users have sent and received).

45. Below is a summary of some of the information contained in the CyberTipline report and the records received from MediaLab.ai Inc. in response to the subpoena and search warrant:

a. The kuru_shinigami444 Kik account was created on or around June 19, 2019. The profile name for the account was "Showgolden".

b. The email address of karate_niidan06@yahoo.com was associated with the account profile. The records identified that this email address had been confirmed or verified by a representative of MediaLab.ai Inc.

c. The account was last accessed on or around December 23, 2020.

d. The Kik account was installed onto a Samsung Android device bearing Model SM-A515U1 on or around September 8, 2020.

e. Approximately nine videos depicting suspected child pornography and/or child exploitation material were located in the kuro_shinigami444 Kik account and reported to NCMEC in the CyberTipline report. The report identified that approximately six of the videos were shared in a messaging group(s) by the kuro_shinigami444 account user, and that approximately three of the videos were sent by the kuro_shinigami444 account user to one (or more) other user(s) via private chat message(s). The report indicated that MediaLab.ai Inc. discovered the approximately nine video files in the kuro_shinigami444 Kik account on or around December 3, 2020.

f. I have reviewed the approximately nine video files that MediaLab.ai Inc. discovered in the kuro_shinigami444 Kik account. Based on my review of the files and my training and experience, I believe that at least approximately six of the videos depict child pornography. I further believe that the remaining approximately three videos depict possible child pornography (i.e., files depicting possible children, although I could not conclude with sufficient certainty if the individuals were in fact minors). By way of example, two of the files depicting child pornography are described as follows:

   i. 6bd8eaa1-7dee-44b7-96f0-405e02cf016d.mp4: The file is a video that depicts what appears to be a nude toddler-aged female child on a bed. What appears to be a white male (whose face is not captured in the video) fondles the toddler's vagina with his hand, masturbates his penis, and rubs his penis on the toddler's vagina. The toddler also touches the male's penis with her hand. The video is approximately one minute and 59 seconds in duration. The log files identified that the kuru_shinigami444 Kik account user distributed this video file to another user via a private chat message on or around November 27, 2020.

   ii. 2d732b33-56d1-4fcc-a9d8-08010ebf9711.mp4: The file is a video that depicts what appears to be a nude pre-pubescent white female child and a nude pre-pubescent white male child. The female child performs fellatio on the male child's penis and fondles his penis with her hand. The video is approximately one minute and 58 seconds in duration. The log files

identified that the kuru_shinigami444 Kik account user distributed this video file to approximately 25 other users via a group chat message on or around November 25, 2020.

g. The log of IP addresses for the account indicated that a number of IP addresses serviced by Verizon and Servers Australia Pty. Ltd. were utilized to access the account.

i. Based on Internet research, it appears that Servers Australia Pty. Ltd. is a VPN provider based in Australia. Their website indicates that the company hosts other VPN providers throughout the world.

ii. Based on my training and experience, I know that the use of IP addresses serviced by Servers Australia Pty. Ltd. is consistent with someone using a VPN to access the Internet. I also know that the use of IP addresses serviced by Verizon is consistent with someone using the data plan from his/her cellular telephone or tablet to access the Internet.

iii. Again based on my training and experience, I know that individuals who utilize VPN's on their computer devices do not always take the time or effort needed to log into the VPN's when accessing the Internet. It is not uncommon for such individuals to sometimes utilize the Internet service from the data plans on their cellular telephones or tablets and/or from the wireless Internet service at their residences.

Records from Oath Holdings Inc.

46. On or around January 12, 2021 and July 14, 2021, Oath Holdings Inc. (the service provider for Yahoo email accounts) was served with administrative subpoenas requesting subscriber information for the karate_niidan06@yahoo.com email account as well as the log of IP addresses that were utilized to access the account. On or around July 28, 2021, a federal search warrant was served to Oath Holdings Inc. requesting information associated with the karate_niidan06@yahoo.com account (to include the contents of the email account). Records received from Oath Holdings Inc. in response to the two administrative subpoenas and the federal search warrant included the following information:

a. The karate_niidan06@yahoo.com account was created on or around December 12, 2006.

b. The user name for the account was "GEORGE GIBBS". The user's birthday was listed as being XX/XX/1988 (redacted for purposes of this Affidavit).

i. This birthday matches GIBBS' date of birth.

c. The telephone number of 937-475-2654 was associated with the account. The records identified that this telephone number had been verified by a representative of Oath Holdings Inc.

d. The account was last accessed on or around July 28, 2021 (the date of the issuance of the search warrant).

e. The log of IP addresses identified that the following IP addresses were utilized to access the account:

   i. IP addresses serviced by Servers Australia Pty. Ltd. and several other providers that also appear to be associated with VPN's;

   ii. IP addresses serviced by the Verizon cellular telephone network; and

   iii. An IP address serviced by AT&T (that being 99.88.157.4).

f. More than 850 email messages were contained in the account. A number of these messages included information indicative that GIBBS is the user of the account. By way of example, some of these messages included the following:

   i. At least approximately 15 of the sent email messages contained "GEORGE GIBBS III", "GEORGE M. GIBBS III", or "G. GIBBS III" in the signature line.

   ii. In or around March 2020, the karate_niidan06@yahoo.com account user exchanged email messages with an individual who appeared (based on the signature line) to be the Director of Human Resources and Risk Management for a company based in California. In the messages, the karate_niidan06@yahoo.com account user requested copies of his prior W2 tax forms. As part of making the request, the karate_niidan06@yahoo.com account user identified that his name was "GEORGE M. GIBBS III", his date of birth was XX/XX/1988 (redacted for purposes of this Affidavit), the last four digits of his social security number were 5717, and that he resided at 2803 Stone Mille Place in Beavercreek, Ohio (hereinafter referred to as the "SUBJECT PREMISES").

      1. The date of birth and last four digits of the social security number that were provided by the karate_niidan06@yahoo.com account user in the email message matches GIBBS' date of birth and social security number. As detailed below, GIBBS uses the SUBJECT PREMISES on his current Ohio driver's license.

g. On or around December 23, 2020, the karate_niidan06@yahoo.com account user received an email message from an email address associated with the CyberGhost VPN provider. The email provided a license key needed to activate a CyberGhost VPN account.

i. As noted above, IP addresses associated with several VPN's were utilized to access the karate_niidan06@yahoo.com email account and the kuru_shinigami444 Kik account.

h. On or around February 20, 2021, approximately four email messages were received by the karate_niidan06@yahoo.com account from an email address associated with the Mega cloud storage provider. The email messages indicated that a Mega account associated with the karate_niidan06@yahoo.com email address had been created on or around February 20, 2021.

i. On or around July 17, 2021, an email message was sent from karate_niidan06@yahoo.com to karate_niidan06@yahoo.com. The only text in the body of the message was a URL that appeared to be associated with a sharing link to a Mega account.

i. Based on my training and experience, I know that individuals sometimes email files and/or URL's to themselves for a variety of reasons, including but not limited to the following: (1) to store the files and/or URL's in a secure location that is outside of their computer devices, (2) to provide a means to access the files and/or URL's on different devices, or (3) in preparation to email the files and/or URL's to others.

ii. As detailed above in the background section of the Affidavit, I know that individuals commonly utilize cloud storage accounts such as Mega to store their files. Also as detailed above, I know that it common for individuals to trade child pornography files by sending sharing links to cloud storage accounts.

Other Subpoenaed Records

47. Verizon was identified as being the service provider for telephone number 937-475-2654. On or around February 4, 2021, Verizon was served with an administrative subpoena requesting subscriber information for this telephone number. Records received from Verizon in response to the subpoena included the following information:

a. The telephone number was subscribed to "GEORGE GIBBS III" at the SUBJECT PREMISES.

b. The account was activated on or around July 3, 2020, and it was active as of the date

of the subpoena.

c. The device that utilized the telephone number was a Samsung A51 bearing Model SM-A515U1-VS.

i. As noted above, the kuro_shinigami444 Kik account was installed on a device bearing the same model on or around September 8, 2020.

48. On or around July 14, 2021 and August 9, 2021, AT&T was served with two administrative subpoenas requesting subscriber information for the IP address of 99.88.157.4 on a sample of four of the dates and times that it was utilized to access the karate_niidan06@yahoo.com email account (four dates during the approximate time period of August 12, 2020 to include July 28, 2021). Records received in response to the subpoena identified that this IP address was subscribed to "GEORGE GIBBS"[2] at the SUBJECT PREMISES. The records further identified that the Internet account was active as of on or around August 2, 2021.

49. On or around August 7, 2021, Mega Ltd. was served with an administrative subpoena requesting subscriber information for any Mega accounts associated with the email address karate_niidan06@yahoo.com as well as the log of IP addresses that were utilized to access the account. Records provided by Mega Ltd. in response to the subpoena included the following information:

a. Consistent with the emails located in the karate_niidan06@yahoo.com email account, a Mega account associated with this email address was created on or around February 20, 2021. The user name for the account was "GEORGE GIBBS".

b. Two IP addresses were utilized to access the account: 98.88.157.4 (the IP address that is subscribed to "GEORGE GIBBS" at the SUBJECT PREMISES) and an IP address that appears to be associated with a VPN.

50. As detailed above, on or around July 17, 2021, the karate_niidan06@yahoo.com account user emailed himself what appeared to be a Mega sharing link. On or around August 7, 2021, Mega Ltd. was served with an administrative subpoena requesting subscriber information for the Mega account that had posted this sharing link, as well as the log of IP addresses that were utilized to access the account. Based on the records provided by Mega Ltd. in response to the subpoena, it did not appear that GIBBS was the user of this account – specifically, the account was associated with an email address and IP addresses that do not appear at this time to be associated with GIBBS. It is therefore reasonable to believe that GIBBS had received this sharing link from another individual.

---

2 As detailed in the subsequent paragraph, it appears GIBBS's father's name is also George Gibbs. It is unknown if GIBBS or his father is the subscriber of the Internet account.

Mega Sharing Link

51. On or around August 5, 2021, I typed the URL to the above noted Mega sharing link (the URL located in the karate_niidan06@yahoo.com email account) into an Internet browser and was routed to a publicly accessible portion of a Mega account. The sharing link contained a total of approximately 505 video files that were saved in approximately nine file folders. No encryption key or password was required to access the video files. The videos primarily depicted pre-pubescent children, teenagers, and young adults engaged in sexually explicit conduct. Based on my review of the files and my training and experience, I believe that at least approximately 267 of the videos depict child pornography. A number of the other videos depict possible child pornography (i.e., files depicting possible children, although I could not conclude with sufficient certainty if the individuals were in fact minors). By way of example, two of the files depicting child pornography are described as follows:

a. (pthc) NEW 2016 Pedo Childlover 8yo Daddy's Little Girl JM 10.mp4: The file is a video that depicts what appears to be a nude pre-pubescent white female child lying on her back with her legs spread apart. What appears to be an adult white male performs cunnilingus on the child. The child sits ups, and the adult male inserts his penis into the child's mouth. The adult male proceeds to masturbate his penis and secrete semen onto the child's vagina. The video is approximately 10 minutes and 43 seconds in duration. The video was saved in a file folder entitled "Eating pussy".

b. VID-20201008-WA0053.mp4: The file is a video that depicts what appears to be a pre-pubescent white female child who is wearing a shirt and a skirt pulled up around her waist but no underwear. The child is lying on her back with her legs spread apart. What appears to be an adult white male engages in vaginal sexual intercourse with the child. The video is approximately 18 seconds in duration. The video was saved in a folder entitled "Cumshot".

Search Warrant at the SUBJECT PREMISES

52. On or around August 23, 2021, search warrants were authorized by the United States District Court for the Southern District of Ohio for the SUBJECT PREMISES and GIBBS' person. Agents and officers of the FBI and the Beavercreek Police Department executed the warrants on or around August 27, 2021. GIBBS, Adult A (GIBBS' father), Adult C (GIBBS' wife), and a juvenile child were present when agents and officers arrived to execute the warrants. Among other items, the following were seized pursuant to the warrants:

a. A Samsung A51 Model SM-A515U1 cellular telephone, which was seized from GIBBS' bedroom;

i. As noted above, the kuro_shinigami444 Kik account was installed on a

device bearing the same model on or around September 8, 2020.

b. An Acer laptop, which was seized from GIBBS' bedroom;

c. A black Western Digital external hard drive, which was seized from a backpack in GIBBS' bedroom;

d. A black and orange PHD 3.0 Silicon-Power portable hard drive, which was seized from a backpack in GIBBS' bedroom; and

e. Two iPhones, which Adult A (GIBBS' father) identified as belonging to him.

53. During the execution of the search warrants, GIBBS agreed to be interviewed after being advised of his Miranda rights. Below is a summary of some of the information provided by GIBBS during the interview:

a. GIBBS resided at the SUBJECT PREMISES with his wife (Adult C); his parents (Adult A and Adult B); and his and Adult C's two juvenile children.

b. GIBBS had a Samsung cellular telephone bearing telephone number 937-475-2654. The telephone was in his bedroom.

c. GIBBS had a laptop computer that was in his bedroom as well a black external hard drive and an orange external hard drive. GIBBS was shown the black Western Digital external hard drive and the black and orange PHD 3.0 Silicon-Power portable hard drive that were recovered from the backpack in his bedroom, and he confirmed that these devices belonged to him.

d. GIBBS utilized the email address karate_niidan06@yahooo.com (the email address associated with the kuru_shinigami444 Kik account).

e. GIBBS began viewing pornography as a child, and he developed a significant addiction to pornography.

f. GIBBS began viewing child pornography in mid- or late-2020 after another individual sent him a child pornography file via the Wickr messenger application. He thereafter developed an addiction to child pornography.

g. GIBBS traded child pornography files with others via the Wickr and Kik messenger applications. His Wickr account name was "showgolden", and his Kik account name was kuru_shinigami444. GIBBS also obtained and viewed child pornography files from the TOR[3] website. He obtained and viewed both images and videos of child

3 The Onion Router (TOR) is a free and open-source software that provides users with anonymous communications and browsing on the Internet. The software directs Internet traffic through a free, worldwide volunteer

pornography depicting children of all ages. GIBBS occasionally utilized the child pornography files to masturbate.

h. GIBBS utilized his Samsung cellular telephone to access his Wickr and Kik accounts. He did not save the child pornography files onto his cellular telephone but rather saved the files to his black external hard drive. He transferred the files from his cellular telephone to his external hard drive by connecting both devices to his laptop.

i. There were times when GIBBS' trading partners sent him child pornography files via sharing links to Mega accounts. GIBBS opened a Mega account utilizing the karate_niidan06@yahoo.com email address so that he could better access these links. GIBBS denied saving any child pornography files to his Mega account.

j. GIBBS sometimes emailed himself the Mega sharing links containing child pornography that he received from others so that he could access the links at later times. GIBBS recalled emailing Mega links to himself in 2020, but he did not recall emailing himself any links in July 2021.

k. GIBBS was "banned" from Kik in December 2020 because child pornography files were found in his account. He attempted to stop viewing child pornography at that time, and he deleted the child pornography files from the black external hard drive. GIBBS later "relapsed" and continued trading child pornography with others on Wickr. He also utilized a computer software program to recover some (but not all) of the child pornography files he had deleted from the black external hard drive.

l. GIBBS last traded child pornography files with others via Wickr a few weeks ago. GIBBS noted that messages and files contained in the Wickr application were automatically deleted from his account after the passage of time based on the security settings, so the child pornography files he obtained a few weeks ago may no longer be in his Wickr account.

m. GIBBS previously operated and was an instructor at a martial arts studio called Japan Karate-do. He closed the studio in 2020 because of the Coronavirus pandemic.

Examination of Computer Devices

54. Pursuant to the search warrant, the Samsung A51 Model SM-A515U1 cellular telephone that was seized from the SUBJECT PREMISES (which GIBBS identified as being the device he utilized to access his Kik and Wickr accounts and to trade child pornography files) was examined. Below is a summary of some of the information recovered during the examination:

overlay network consisting of more than seven thousand relays. This network conceals a user's location and usage from anyone conducting network surveillance or traffic analysis.

a. The telephone number for the device was 937-475-2654 (the number that GIBBS identified as being his telephone number).

b. The karate_niidan06@yahoo.com email account was established on the telephone.

c. The Wickr application was installed on the telephone. An account with a user name of "showgolden" was logged into on the application. No messages were saved in the account that contained child pornography files. However, it was noted that the showgolden account user had contacts saved in the account for other users with the following account names: "childporn", "youngporn", "loli"[4], "kiddyporn", and "loligirl". On or around August 23, 2021, the showgolden account user sent messages to the "childporn", "youngporn", and "loli" account users inquiring about whether or not their accounts were still active.

d. Consistent with the information provided by GIBBS, no child pornography files were recovered from the device during the preliminary examination.

e. At least approximately four documents were saved on the telephone that contained GIBBS' name on them.

55. Also pursuant to the search warrant, the black Western Digital external hard drive (which was the device that GIBBS identified that he used to save his child pornography files) was examined. Below is a summary of some of the information recovered during the examination:

a. Recovered from the device were approximately 396 images and approximately 635 videos depicting child pornography. Many of the child pornography files were saved in various sub-folders contained within a folder entitled "Black", a subfolder entitled "The Stash", another subfolder entitled "Extras", and another subfolder entitled "Child Porn". By way of example, two of the files depicting child pornography are described as follows:

i. Playing with Toddler Daughter.mp4: The file is a video that depicts what appears to be a nude toddler-aged white female child. The child is first depicted standing nude in a room. The child is then depicted in a bathtub with what appears to be a nude adult white male. The child touches the adult male's penis and performs fellatio on the adult male. The child also stands up at one point, and the camera zooms in on her vagina and buttocks. The

4 "Lolita", sometimes shortened to "loli", is often used as a term to refer to prepubescent or adolescent female children who are attractive and sexually promiscuous. The term originated from a novel about an affair between a man and his 12-year old stepdaughter. Based on my training and experience, I know that "Lolita" and "loli" are search terms that individuals sometimes utilize to search for child pornography files.

child and adult male are then depicted in another setting. The child again performs fellatio on the adult male. The adult male masturbates his penis and secretes semen onto the child's vagina and abdomen. The video ends by displaying the following text: "Aint I good to you lol…….". The video is approximately three minutes and 36 seconds in duration.

ii. Daddy Touched Daughter During Diaper Change.mp4: The file is a video that depicts what appears to be a nude toddler-aged white female child. Another individual removes the child's diaper and digitally penetrates her vagina. The video is approximately one minute and 27 seconds in duration.

b. Saved on the device were approximately 495 of the 505 files that I observed in and downloaded from the Mega sharing link noted above (the link contained in the email message sent to and from the karate_niidan06@yahoo.com account on or around July 17, 2021). The files were saved in the same nine folders as those contained in the Mega sharing link. The metadata for the files identified that the files from approximately four of the folders were saved onto the external hard drive on or around July 17, 2021, and that files from approximately five of the folders were saved onto the external hard drive on or around July 19, 2021.

c. A number of images and videos depicting GIBBS were saved on the device.

56. Also pursuant to the search warrant, the black and orange PHD 3.0 Silicon-Power portable hard drive (which GIBBS identified as belonging to him) was examined. Below is a summary of some of the information recovered during the examination:

a. Recovered from the deleted space of the device were approximately 9,519 images and approximately 820 videos depicting child pornography. By way of example, two of the files depicting child pornography are described as follows:

i. File with hash value of 6e3536f5d266c21ef89afc6517ce4830c0beb16e: The file is an image that depicts what appears to be a white toddler-aged female child who is wearing a dress but no pants or underwear. The child has a pacifier in her mouth. The child is lying on her back with her legs straddled, and what appears to be an adult white male's penis is inserted into her anus.

ii. File with hash value of 33937da4ebe825b1b1f589cfd38d8e78255d7902: The file is an image that depicts what appears to be a nude pre-pubescent white female child. The child is hung upside down from a rope, and a bandana is covering her eyes. An object is inserted into the child's vagina.

b. A number of images and videos depicting GIBBS were saved on the device.

57. Again pursuant to the search warrant, the Acer laptop (the device that GIBBS identified that

he used to transfer his child pornography files from his cellular telephone to his external hard drive) was examined. Below is a summary of some of the information recovered during the examination:

a. Various artifacts were recovered during the examination that were indicative that GIBBS was the user of the laptop. For example, images and videos depicting GIBBS, a resume with GIBBS' name on it, and an application for a Social Security Card with GIBBS' name on it were saved on the laptop. Also by way of example, over one thousand four hundred artifacts were recovered from the laptop that included the email address karate_niidan06@yahoo.com.

b. At least approximately 864 images depicting child pornography were recovered from the laptop. The child pornography files were recovered from a file path that stores thumbnail images for files that have been viewed on the laptop and from the deleted space of the laptop. By way of example, two of the files depicting child pornography are described as follows:

   i. File with a hash value of 50b29fc56b0fd517319496aad7542e862a65301a: The file is an image that depicts what appears to be a nude pre-pubescent white female child kneeling on what appears to be a bed. What appears to be an adult white female is spreading apart the child's buttocks and licking (or close to licking) the child's anus.

   ii. File with a hash value of e6af169607df33b285833ab4132cb11c1b410a27: The file is an image that depicts what appears to be a nude pre-pubescent white female child lying on what appears to be a board or table. The child is bound to the board or table with a white rope. What appears to be a nude adult white male is standing over the child, and his penis is in the child's mouth.

c. Various artifacts were recovered from the computer that included file names and file folder names matching those from the Mega sharing link noted above (the link contained in the email message sent to and from the karate_niidan06@yahoo.com account on or around July 17, 2021). Although the files themselves were not saved on the laptop, the artifacts were indicative that a number of those files and file folders had been accessed and/or viewed on the laptop during the approximate time period of July 17, 2021 through July 19, 2021 (which is consistent with the dates that the files were saved onto the Western Digital external hard drive). Some of the artifacts were also indicative that at least some of the files from the Mega sharing link were previously saved on the desktop of the laptop in a folder entitled "DESTROY ASAP" and a subfolder entitled "Hetero".

d. A cellular telephone with a name of "George's Galaxy A51" (consistent with GIBBS' Samsung cellular telephone) and a Western Digital external hard drive with

a serial number matching that of the device seized from the backpack in GIBBS bedroom had both been attached to the laptop as recently as on or around August 10, 2021.

i. This information is consistent with GIBBS utilizing his laptop to transfer his child pornography files from his Samsung cellular telephone to his Western Digital external hard drive.

58. The two iPhones that GIBBS' father identified as belonging to him were examined. No child pornography files were recovered from these two devices.

Arrest and Conviction of GIBBS

59. Based on the information detailed above, there is probable cause to believe that GIBBS was the user of the following in 2021:

a. The kuru_shinigami444 Kik account;

b. The showgolden Wickr account;

c. The Samsung A51 Model SM-A515U1 cellular telephone bearing telephone number 937-475-2654 that was recovered from GIBBS' bedroom at the SUBJECT PREMISES;

d. The black Western Digital external hard drive and PHD 3.0 Silicon-Power portable hard drive that were recovered from GIBBS' bedroom at the SUBJECT PREMISES; and

e. The Acer laptop that was recovered from GIBBS' bedroom at the SUBJECT PREMISES.

60. There is also probable cause to believe that GIBBS committed the following violations in 2021:

a. GIBBS utilized his Samsung cellular telephone and his Kik and Wickr accounts to distribute child pornography.

b. GIBBS received and downloaded child pornography files from Mega sharing links.

c. GIBBS utilized his Western Digital external hard drive, PHD 3.0 Silicon-Power portable hard drive, and Acer laptop to possess and access with the intent to view child pornography files.

61. On or around September 14, 2021, Magistrate Judge Sharon L. Ovington signed a Criminal Complaint and arrest warrant charging GIBBS with two counts of distribution of child pornography, in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1); two counts of receipt of child pornography, in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1); and one count of possession of child pornography, in violation of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2).

62. On or around September 15, 2021, GIBBS came to the FBI's office in Centerville, Ohio at my request. Upon his arrival, GIBBS was taken into custody pursuant to the arrest warrant. Several items of personal property were collected from GIBBS' person, including a Samsung cellular telephone bearing model SM-S111DL[5] and an IMEI number of 352319150023008. Pursuant to GIBBS' consent, these items were released to his father later that day.

63. On or around September 20, 2021, a detention hearing was held for GIBBS before Magistrate Judge Ovington. Magistrate Judge Ovington ordered GIBBS to be released pursuant to home detention and electronic monitoring pending the resolution of the criminal case. As part of the terms of his release, GIBBS was forbidden from accessing any computer devices capable of accessing the Internet and any sexually explicit materials. GIBBS was released from custody on or around September 24, 2021.

64. On or around September 28, 2021, an indictment was returned in the United States District Court for the Southern District of Ohio charging GIBBS with three counts of distribution of child pornography, in violation of 18 U.S.C. §2252(a)(2) and (b)(1); one count of receipt of child pornography, in violation of 18 U.S.C. §2252(a)(2) and (b)(1); and one count of possession of child pornography, in violation of 18 U.S.C. §2252(a)(4)(B) and (b)(2). On or around March 14, 2022, GIBBS pled guilty to one count of possession of child pornography, in violation of 18 U.S.C. §2252(a)(4)(B) and (b)(2).

65. I have spoken to the officer from the United States Pretrial Services Office who currently supervises GIBBS. This officer informed me of the following information:

a. GIBBS has resided at the SUBJECT PREMISES from the time that he was released from custody in September 2021 through the present. Pretrial Services officers have conducted periodic home visits and have confirmed that GIBBS resides at the SUBJECT PREMISES.

b. GIBBS and his father are the only individuals who currently reside at the SUBJECT PREMISES. GIBBS' mother, wife, and children have all moved out of the

5 The model number that was documented by the officer who completed the property receipt was SM-111DL. From Internet research, I know that there is a Samsung cellular telephone bearing model number SM-S111DL, but that there are no Samsung cellular telephones with a model number of SM-111DL (i.e., without the "S" in front of the 111DL). Internet research of the IMEI number for the cellular telephone identified that the telephone was a Samsung device bearing model SM-S111DL. Therefore, it appears that the officer committed a transcriptionist error when writing down the model number.

residence.

c. GIBBS has not received authorization to utilize any electronic devices. He is supposed to use the home's landline telephone when making any telephone calls.

Post-Arrest Activity on Kik Messenger

66. Throughout 2022, agents and investigators of the Salt Lake City, Utah division of the FBI have conducted online investigations to identify individuals utilizing social media and messenger applications to commit child exploitation offenses. As part of these investigations, an FBI online covert employee (hereinafter referred to as "OCE") routinely accessed group chats that promoted the distribution and receipt of child pornography.

67. On or around March 12, 2022, OCE was invited into a group chat on the Kik messenger application by another group member. This group had a user name of "**#underfifteen**" and a profile name of "You know". OCE briefly participated in this group chat and exchanged private messages with two of the group's administrators. OCE observed child pornography files being distributed in the group. Below is a summary of OCE's communications and observations while he was in the group and communicated with the administrators:

a. Upon entering the group, OCE observed a standard message that detailed the rules of the group. These rules identified that in order to be accepted into the group, users must do the following: (1) identify their "ASL" (a term to refer to age, sex, and location) upon two minutes of entering the group, and (2) send one of the group's administrators a "PM" (a term to refer to a private message) with two pictures or one video depicting "young" content. Various other rules were detailed, including a rule that the "oldest talkers" were at risk of being removed from the group.

i. Based on my training and experience, I know that administrators of groups that trade child pornography on messenger applications such as Kik often require that users send child pornography files in order to be accepted into the groups. The administrators also often remove members who are not actively sharing child pornography files. These practices are enforced as a means to prevent law enforcement officers from entering and/or remaining in the groups and to ensure that everyone is contributing to the supply of child pornography files.

b. Four administrators were identified for the group, including one with a user name of **Sentai_Sensei**[6] and a profile name of "GEO The Banhammer"[7] and another with a

6 Sensei is a term to refer to a teacher or instructor, usually of a Japanese martial arts studio. As noted above, GIBBS previously was an instructor at a martial arts studio.

7 Banhammer is a term to refer to the power of moderators and system administrators to ban users from digital space.

user name thebestone1985 and a profile name of "Naughty Screwdriver". The above detailed message identified that if none of the administrators were available to verify a new user, the user should send his/her files to the **Sentai_Sensei** user. OCE observed that the profile picture for the **Sentai_Sensei** account user was a picture of a person wearing a black hood and a mask. The background picture for the **Sentai_Sensei** account user was a picture of the torso and legs of a white male who was wearing only underwear and was lying on a bed.

i. Administrators of Kik groups have the ability to create groups, invite or remove members, and create rules for the group. However, a current administrator may or may not be the person who created the group.

c. OCE observed that approximately 100 Kik users were in the **#underfifteen** group.

d. After entering the **#underfifteen** group, OCE initially purported himself to be a 16-year old female. OCE asked who he should private message to provide his verification files. The Kik user with the user name of thebestone1985 and a profile name of "Naughty Screwdriver" instructed OCE to message him.

e. OCE sent a private message to the thebestone1985 account user and sent this user a picture that OCE purported to be of himself (posing as the 16-year old child). The thebestone1985 account user responded that this picture was not what OCE was supposed to send and instructed OCE to contact "geo" (referring to the **Sentai_Sensei** Kik account user with the profile name of "GEO The Banhammer").

f. OCE sent a private message to the **Sentai_Sensei** Kik account user. OCE and the **Sentai_Sensei** account user had the following discussion:

i. The **Sentai_Sensei** account user said that the way that OCE had entered the Kik group was a violation of the group's rules.

ii. OCE sent the **Sentai_Sensei** account user a picture of a purported female child. The **Sentai_Sensei** account user told OCE that verification files for the group typically involved pictures or videos of "young content, meaning CP". The **Sentai_Sensei** account user further advised that the group only accepted things like "young nudes or something close to it".

1. "CP" is a common term to refer to child pornography.

iii. OCE told the **Sentai_Sensei** account user that he was not actually a 16-year old female child but rather was a 38-year old male who had a 16 year old daughter. OCE commented that he was looking to trade files with other parents.

iv. The **Sentai_Sensei** account user told OCE that the group was intended for sharing files, not trading files. The **Sentai_Sensei** account user also said that because OCE was untruthful about his "ASL" (age, sex, and location), OCE had violated the group's rules. The **Sentai_Sensei** account user told OCE that he needed to leave the group.

g. While in the **#underfifteen** group chat, OCE observed the thebestone1985 account user posted three video files into the group chat. Based on my training and experience, I believe that at least two of the videos depict child pornography. I further believe that the third video depicts possible child pornography (i.e., a file depicting a possible child, although I could not conclude with sufficient certainty if the individual was in fact a minor). The two files depicting suspected child pornography are described as follows:

i. RYMG8216.mp4: The file is a video that depicts what appears to be a nude adult white male having vaginal sexual intercourse with what appears to be a nude white or Hispanic female child. The video is approximately 21 seconds in duration.

ii. JQHC9716.mp4: The file is a video that depicts what appears to be a nude white male and a pre-pubescent white female child who is wearing clothing. The two individuals are sitting next to each other. The white male reaches into the child's shorts, and it appears that he fondles her vagina. The female child also uses her hand to masturbate the male's penis. The video is approximately two minutes in duration.

h. After the three videos noted above were sent, the **Sentai_Sensei** account user stated the following, which appeared to be directed to OCE: "Verification unsuccessful". OCE then received a notification that he had been removed from the group.

i. Below are excerpts from the communications in the **#underfifteen** group chat and the private messages that were exchanged with the **Sentai_Sensei** and thebestone1985 account users:

Group Chat:

Initial Standard Message:

STOP

If you do not have a profile picture on your account, put one on BEFORE anything else. You will not be verified without one.

Welcome! Say hello to everybody and state your ASL within 2 minutes upon entry or you WILL be automatically removed.

TO VERIFY you will be asked to PM either TWO pictures or ONE video featuring "young" content to the active VERIFYING ADMIN. They will share your content with the rest of the group to confirm your verification.

Verifying Admins
GEO (@**Sentai_Sensei**);
Jasmine (@jazzybear2021);
naughty (@thebestone1985);
princess (@prinxessbubble5).

Content Moderators
GEO "THE BANHAMMER"
Jasmine
Mike Stevens
ameli Holzer

GROUP RULES:
1) Share whatever you want, no age limits. However, NO hardcore rape, or any other material that could be considered violent, portray discomfort, pain, crying, or you will be banned from the group upon discovery. If you have questions about what you are allowed to share, please consult with an active admin
2) NO TRADING! Please share with the group. If you can't share yet ask an active admin to share for you
3) DO NOT post advertisements of any kind before you're verified or you will be banned
4) DO NOT invite users without consulting with an active admin
5) No links to other groups are allowed in main chat
6) DO NOT PM ANYONE without prior consent from the member you are trying to contact
7) Dont be mean, this chat isn't for fighting
8) KEEP ACTIVE! Oldest talkers have a risk of being removed

ADDITIONAL UPDATES:
1) If an admin is not currently available to verify, send your verifications to GEO "THE BANHAMMER" and he will get to them upon returning. If you fail to do so you will be removed no questions asked.
2) The following words are now forbidden to use in chat and will result in you being BANNED if said:

TRADE, CRY, RAPE, ABUSE, TORTURE, or any racist language.
This is a potentially incomplete list and is subject to change.

OCE:	Hello
OCE:	16 f Utah
Rebel1030:	Hey there
OCE:	Who do I PM?
thebesttone1985:	Pm me
Sentai_Sensei:	Hannah, can I have a word with you?
thebesttone1985:	And verify with me
Rebel1030:	Hannah?
Sentai_Sensei:	Activity
Unknown User:	*Posts information regarding other users' account activities*
Sentai_Sensei:	Are you still working that verification naughty?
thebesttone1985:	Yea
thebesttone1985:	*Sends video depicting possible child pornography*
thebesttone1985:	From rebel
thebesttone1985:	*Sends video depicting child pornography*
thebesttone1985:	*Sends video depicting child pornography*
thebesttone1985:	Also from rebel
Rebel1030:	Thank you
Sentai_Sensei:	Verification unsuccessful
OCE:	*Receives message stating: "You have been removed from the group"*

<u>Private Messages with thebesttone1985 Account User:</u>

OCE:	Hello
thebesttone1985:	Hi to verify I need 2 pics or 1 vid of young content plz
OCE:	Of me?
OCE:	*Sends image of a clothed female*
thebesttone1985:	No
thebesttone1985:	Read the sec part of the rules k
OCE:	Ok
thebesttone1985:	Hey pm geo plz u have 2 mins
OCE:	Ok

<u>Private Messages with **Sentai_Sensei** Account User:</u>

OCE:	Hey
OCE:	*Sends image of a clothed female*
Sentai_Sensei:	Hello, I asked naughty to have you contact me because the way you entered the chat was actually violation of Rule #4, but it wasn't your fault. I saw that you were invited in by

	Hannah J. We don't typically allow people in to the group that were invited by other members, that's to help control the climate here. I'm trying to reach Hannah to discuss that with her so if you can just standby for a moment please?
OCE:	Ok
OCE:	I have a 16 yo female
Sentai_Sensei:	Ok, sorry about that. So verifications for this group are typically pictures or videos of young content, meaning cp. Do you understand what this group is for first off?
OCE:	Yes other parents with yung kids to trade Original Content or live
OCE:	Mainly parents active in yung incest mmmmmm
OCE:	Is that fine?
Sentai_Sensei:	So as far as verification content is concerned, we only accept things like young nudes or something close to it. They are also shared into the chat to validate the verification. Do you understand that?
OCE:	Yes I do, but I want a fair trade of my 16 yo dau with someone else. If this isn't a parent group active with their yung ones I totally understand maybe it's not the right group for me. I'm just a horny perv dad lol
OCE:	Just looking for like minded pervs
Sentai_Sensei:	Ok, so the ASL that you posted in chat was false?
OCE:	No I have a 16 yo f in Utah. That's where I live and hoping that there is a local parent as well
Sentai_Sensei:	But your OWN asl is that of an older male, is that accurate?
OCE:	Yes sorry. I'm a 38 yo dad with a 16 yo dau
OCE:	Sorry for the confusion
Sentai_Sensei:	Ok, so you are in the wrong kind of group. This is not a trading group at all to begin with, only a sharing group. So because you weren't truthful about the ASL in chat, I need to ask you to respectfully leave
OCE:	No worries brother. Happy hunting. Let me know if you find a dad or mom out there having sex with their little ones.

<u>Subpoenas Issued in 2022</u>

68. On or around March 15, 2022, MediaLab.ai Inc. was served with an administrative subpoena requesting subscriber information for the **Sentai_Sensei** Kik account as well as the log of IP addresses that were utilized to access the account. Records received from MediaLab.ai Inc. in response to the subpoena included the following information:

a. The **Sentai_Sensei** Kik account was created on or around September 12, 2021.

i. It was noted that the Kik account was created approximately 16 days after the search warrant was executed at the SUBJECT PREMISES on or around August 27, 2021.

b. The current profile name for the account was "GEO". However, the profile name had been changed on several occasions.

c. The email address of **sentai.sensei@gmail.com** was associated with the account. The records identified that this email address had not been confirmed or verified by a representative of MediaLab.ai Inc.

d. The Kik account was utilized on a Samsung Android device bearing Model SM-S111DL on or around March 17, 2022.

i. It was noted that this make and model of an Android device matches the make and model of the cellular telephone that GIBBS brought with him to the FBI office when he was arrested on or around September 15, 2021. As noted above, this telephone was released to GIBBS' father.

e. The user's birthday was listed as being XX/XX/1988 (redacted for purposes of this Affidavit).

i. This birthday matches GIBBS' date of birth.

f. The log of IP addresses utilized to access the account was provided for the time period of September 12, 2021 through March 17, 2022. Review of the log provided the following information:

i. The account was accessed on a total of approximately 13,024 occasions as follows:

1. On approximately 36 occasions during the approximate time period of September 12, 2021 through September 13, 2021;

2. On approximately one occasion on or around September 29, 2021 (approximately five days after GIBBS was released on bond following his arrest for the child pornography charges); and

3. On approximately 12,987 occasions during the approximate time period of January 27, 2021 through March 17, 2021 (on a daily basis, multiple times per day, for the entire time period).

ii. The IP address of 99.88.157.4 was utilized to access the account on approximately 7,033 occasions.

1. This is the same IP address that was utilized in 2021 to access the karate_niidan06@yahoo.com account, and which was subscribed to "GEORGE GIBBS" at the SUBJECT PREMISES (as detailed above).

2. This was the only IP address that was utilized to access the account on or around March 12, 2022 (the date that OCE participated in the **#underfifteen** group chat and communicated directly with the **Sentai_Sensei** Kik account user).

3. This IP address was utilized to access the account as recently as on or around March 14, 2022.

iii. A number of IP addresses serviced by the Verizon cellular telephone network were utilized to access the account on approximately 5,540 occasions.

iv. A number of IP addresses that appear to be associated with VPN's were utilized to access the account on approximately 451 occasions.

69. On or around March 23, 2022, AT&T was served with an administrative subpoena requesting subscriber information for the IP address of 99.88.157.4 on March 12, 2022, on one of the times that it was utilized to access the **Sentai_Sensei** Kik account. Records received from AT&T in response to the subpoena identified that the IP address was subscribed to "GEORGE GIBBS" at the SUBJECT PREMISES.

70. Also on or around March 23, 2022, Google LLC was served with an administrative subpoena requesting subscriber information for the **sentai.sensei@gmail.com** Google account, as well as the log of IP addresses utilized to access the account. Records received from Google LLC in response to the subpoena provided the following information:

a. The account was created on or around September 5, 2021.

i. It was noted that the account was created approximately nine days after the search warrant was executed at the SUBJECT PREMISES on or around August 27, 2021, and approximately seven days before the **Sentai_Sensei** Kik account was created.

b. The user name for the account was "GEORGE GIBBS".

c. The telephone number associated with the account was 937-271-3364.

d. The log of IP addresses utilized to access the account was provided for the time period of January 27, 2022 through March 7, 2022. Review of the log provided the following information:

i. The account was accessed on a total of approximately eight occasions.

ii. The IP address of 99.88.157.4 (the IP address subscribed to "GEORGE GIBBS" at the SUBJECT PREMISES) was utilized to access the account on approximately one occasion.

iii. Dynamic IP addresses serviced by AT&T were utilized to access the account on approximately four occasions.

iv. IP addresses serviced by the Verizon cellular telephone network were utilized to access the account on approximately three occasions.

71. On or around March 24, 2022, Verizon was served with an administrative subpoena requesting records of all telephone numbers that connected to a sample of three of the IP addresses that had been utilized to access the **Sentai_Sensei** Kik account on the dates and times that those IP addresses had accessed the account. Records received from Verizon in response to the subpoena identified that telephone number 937-271-3364 (the telephone number associated with the **sentai.sensei@gmail.com** Google account) had connected to all three of the IP addresses on the dates and times listed in the subpoena.

72. On or around April 20, 2022, Verizon was served with an administrative subpoena requesting subscriber information for telephone number 937-271-3364 (the telephone number associated with the **sentai.sensei@gmail.com** Google account). Records received from Verizon in response to the subpoena provided the following information:

a. The telephone had been sold by TracFone (a reseller of cellular telephones), and no subscriber information was maintained for the account.

b. The telephone number was activated on or around September 3, 2021 (approximately seven days after the execution of the search warrant at the SUBJECT PREMISES). The account was presently active.

c. The device utilizing the cellular telephone number was a Samsung Model SM-S111DL telephone bearing an IMEI number of 352319150023008.

i. The make and model of the cellular telephone matches the Android device that was used to access the **Sentai_Sensei** Kik account on or around March 17, 2022.

ii. The make, model, and IMEI of the cellular telephone matches the device that GIBBS brought with him to the FBI office when he was arrested on or around September 15, 2021.

Review of Social Media Accounts

73. On or around April 15, 2022, an FBI investigator searched publicly available information on various social media websites and messenger applications for any possible accounts associated with the email address **sentai.sensei@gmail.com** and the telephone number 937-271-3364. The analyst located a WhatsApp account (an encrypted messenger application) associated with telephone number 937-271-3364.

    a. Based on my training and experience, I know that individuals involved in child pornography offenses often utilize encrypted messenger applications such as WhatsApp to trade child pornography files.

74. Also on or around April 15, 2022, an FBI investigator searched various social applications for other social media accounts with a user name of **Sentai_Sensei**. An Instagram social media account with an account name of **Sentai_Sensei** was located. The publicly available account information identified that the profile name for the account was "GEORGE GIBBS III". The profile picture for the account was an image depicting GIBBS holding his son.

Conclusion Regarding New Accounts

75. Based on all of the information detailed in the Affidavit, there is probable cause to believe that GIBBS is the user of the following:

    a. The **Sentai_Sensei** Kik account;

    b. The **sentai.sensei@gmail.com** Google account; and

    c. The Samsung Model SM-S111DL cellular telephone bearing telephone number 937-271-3364.

76. There is also probable cause to believe the following:

    a. GIBBS has utilized his Samsung cellular telephone and the **Sentai_Sensei** Kik account to distribute and receive child pornography files.

    b. GIBBS has administered the **#underfifteen** Kik group. Within this group, GIBBS has conspired with others to distribute and receive child pornography files.

Evidence Available in Email and Social Media Accounts

77. In my experience, individuals often post information on their social media accounts about other electronic accounts that they utilize – including their email addresses, other social media accounts, and messenger accounts (including Kik). This information may provide

evidentiary value to child exploitation investigations in that they help in identifying other accounts utilized by the offenders in furtherance of their child exploitation activities.

78. Based on my training and experience, I am aware that individuals involved in child exploitation schemes often communicate with others involved in similar offenses about their victims and sexual activities via e-mail, social media accounts, and online chat programs (including Kik). I have seen examples of cases where such individuals have communicated with other child predators about their sexual fantasies and prior sexual activities with juveniles. I have also seen cases where such individuals have communicated with others about their remorse and regret for their activities. Both types of communications provide material evidence in child exploitation cases in that they provide admissions of guilt.

79. Also in my experience, individuals involved in child exploitation schemes often utilize email, social media, and online chat programs (including Kik) as a means to locate and recruit victims. They then use the chat functions on these and other websites, as well as email accounts, to communicate with their victims. Such communications provide a means of anonymity to protect the subjects' identities and to conceal the communications from the victims' parents.

80. Based on my training and experience, I know that individuals involved in child pornography offenses often obtain and trade images with each other via a variety of means, including email, social media accounts, photo sharing services, and online chat programs (including Kik and Skype). Individuals also often attempt to obtain child pornography from a variety of sources, including from those with whom they communicate via email, social media sites, Internet chat programs, Internet bulletin boards, Internet Peer-to-Peer file sharing programs, Internet websites, and other sources. I have also seen a number of cases in which individuals email files containing child pornography to themselves – either from one email account to another or from and to the same email account – in order to transfer the files from one electronic device to another.

81. Based on my training and experience, one or more aliases are often used by individuals involved in child exploitation offenses as a means to avoid detection from law enforcement. It is not uncommon for such offenders to create multiple identities, sometimes involving different ages and genders. Offenders sometimes fictitiously portray themselves as juveniles as a means to gain trust and rapport with victims. Offenders also sometimes obtain photographs of other individuals from the Internet to use as their profile pictures and/or to send to the victims.

82. Based on my training and experience, I know that many social media accounts, Internet websites, and telephone providers require users to provide their email accounts when registering for the accounts. The social media and Internet account providers then send the users various notifications regarding messages from other users, information accessed by users, information available by the websites, and other information. Telephone providers often send bills to their customers via email. These messages can provide material evidence

in cases involving child exploitation offenses because they help in identifying what social media, Internet accounts, and telephone account that were utilized by the subjects to communicate with other subjects and victims and what accounts were utilized by the subjects to find child pornography. In addition, the messages help in identifying the identities of other subjects and victims.

83. Based on my training and experience, I know that providers of cellular telephone service and Internet Service Providers typically send their customers monthly billing statements and other records. These statements and records are sometimes mailed to the customers' billing addresses and other times are emailed to the customers' email accounts. These documents can be materially relevant to investigations of child pornography and child exploitation offenses in that they provide evidence of the Internet and cellular telephone accounts utilized in furtherance of the crimes.

84. Also as noted above, email providers maintain various subscriber and user information that their users provide when registering for its accounts. Some email providers also require payment for certain services or features. Such information is materially important in cases where online accounts are utilized to trade child pornography, as this information can help in confirming the identities of the individuals using the accounts and committing the offenses.

85. Email providers maintain various logs of IP addresses utilized to access the accounts. The IP information is again materially important in child pornography investigations. This information helps in identifying the subjects and the locations where their computer devices are located.

Evidence Sought in Other Google Accounts

86. As detailed above, there is probable cause to believe that GIBBS has a Google account associated with the email address **sentai.sensei@gmail.com**.

87. Google LLC has the ability to maintain information associated with the Web and Application history of its users. Such information is materially relevant in child exploitation investigations, as it may help in identifying websites used by subjects to obtain child pornography and locate victims.

88. Google Drive and Google Photos provide users with cloud computing and online file storage (as detailed above) and photo storage services. In my experience, individuals with large collections of child pornography may utilize cloud computing and online storage accounts as a means to store their files after their hard drives become full. In addition, individuals utilize these services as a means to conceal their files from others, including law enforcement.

89. Google Android Backup provides users with the ability to backup data on their cellular telephones and other electronic devices. Such data can be materially relevant in cases in

which cellular telephones and other electronic devices are used to commit child exploitation offenses, as this data may provide historical records of their criminal activities that are no longer saved on the devices.

90. As detailed above, Google Location History is an application in which Google utilizes various data such as cell site information and Wi-Fi routers to locate and geo-locate a cellular telephone device. Google collects and stores this data if the application is enabled by the user, either during the set-up of the device or through the device's settings.

91. Based on my training and experience, I know that location information from cellular telephones and Google accounts can be materially relevant in investigations involving child pornography and child exploitation offenses. This information provides evidence of the travels undertaken by the subject when meeting with possible victims. Data regarding the subjects' whereabouts as obtained from location information can corroborate statements made by the subjects and victims and provide evidence of the locations where the criminal activities took place.

92. In addition, location data regarding the subjects' daily and routine whereabouts, as obtained from Google Location History information and other location data (such as IP logs and cell site records), is often materially relevant in investigations of child pornography and child exploitation offenses. This information can help in identifying the locations of the subjects' primary residences, locations where they routinely frequent, and locations where they maintain their belongings (such as storage units). All of these locations may lead to the identification of the places where the computer devices used in furtherance of the crimes, as well as other evidence of the crimes, may be present. Information regarding the subjects' daily and routine whereabouts may also lead to the identification of co-conspirators and other victims.

93. Most Electronic Service Providers who maintain location information for accounts (including Google LLC) will not analyze the records to provide data specific to particular locations and activities. Furthermore, all locations relevant to the investigation may not be known at the time that the records are requested from and produced by the providers. For example, information obtained pursuant to additional interviews and/or records obtained pursuant to search warrants may lead to the identification of new victims and new criminal conduct. As such, location information is requested from the providers for the entire time period relevant to the investigation. Only information relevant to the investigation of the child pornography and child exploitation offenses will be seized (as further detailed below).

<u>Conclusion Regarding Probable Cause</u>

94. Based on all of the information detailed above, there is probable cause to believe that information associated with the following accounts may contain evidence of GIBBS' child pornography offenses:

a. The Google account **sentai.sensei@gmail.com**;

b. The Kik account with the user name of **Sentai_Sensei** and the Kik group with the group name of **#underfifteen**.

ELECTRONIC COMMUNICATIONS PRIVACY ACT

95. I anticipate executing the requested warrants for the listed account under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrants to require MediaLab.ai Inc. and Google LLC to disclose to the government copies of the records and other information (including the contents of communications) particularly described in Section I of Attachments B-1 and B-2. Upon receipt of the information described in Section I of Attachments B-1 and B-2, government-authorized persons will review that information to locate the items described in Section II of Attachments B-1 and B-2.

CONCLUSION

96. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; and/or property designed for use, intended for use, or used in committing a crime of violations of federal law, may be located in the accounts described in Attachments A-1 through A-5, including the following offenses: 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2), 2252A(a)(5)(B) and (b)(2), 2252(a)(2) and (b)(1), and 2252A(a)(2) and (b)(1).

97. I, therefore, respectfully request that the attached warrants be issued authorizing the search and seizure of the items listed in Attachments B-1 and B-2.

98. Because the warrants for the accounts described in Attachments A-1 and A-2 will be served on MediaLab.ai Inc. and Google LLC, who will then compile the requested records at times convenient to those entities, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

Andrea R Kinzig

Special Agent Andrea R. Kinzig
Federal Bureau of Investigation

SUBSCRIBED and SWORN
before me this 22 of April 2022

HONORABLE MICHAEL J. NEWMAN
UNITED STATES DISTRICT COURT JUDGE

ATTACHMENT A-1

Information associated with the Google account associated with the email address **sentai.sensei@gmail.com** that is stored at premises controlled by Google LLC, a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT B-1
Particular Things to be Seized

I. Information to be disclosed by Google LLC (the "Provider")

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, including any e-mails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-1 for the time period of September 5, 2021 through the present:

1. Subscriber Information: Any available subscriber information for the account, including the following: user-provided name; account email address; account status; Google services used by account; recovery email and SMS recovery number; account creation date and time; terms of service IP address, date, and time; language; Google Account ID ; last logins to the account, including IP address, date, and time; and accounts associated with a particular device, SMS recovery number, IMEI, or Android ID.

2. IP Logs: Logs of IP addresses utilized to access the Google account.

3. Gmail: The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails.

4. Contacts: Any records pertaining to the user's contacts, including: address books; contact lists; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history.

5. Calendar: Any records pertaining to the user's calendar(s), including: Google Calendar events; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history.

6. Messaging: The contents of all text, audio, and video messages associated with the account, including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history.

7. Google Drive and Google Keep: The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes and note titles, lists, and other data uploaded, created, stored, or shared with the account including drafts and deleted records; third-party application data

and backups; SMS data and device backups; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, other Google service (such as Google Classroom or Google Group), or third party application associated with each record; and all associated logs, including access logs and IP addresses, of each record.

8. <u>Photos</u>: The contents of all media associated with the account in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses.

9. <u>Maps</u>: All maps data associated with the account, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; My Maps data; accounts and identifiers receiving or sending Location Sharing information to the account; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history.

10. <u>Location History</u>: All Location History and Web & App Activity indicating the location at which the account was active, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car), and associated logs and user settings, including Timeline access logs and change and deletion history.

11. <u>Chrome and My Activity</u>: All Internet search and browsing history, and application usage history, including Web & App Activity, Voice & Audio History, Google Assistant, and Google Home, including: search queries and clicks, including transcribed or recorded voice queries and Google Assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant. Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, the Provider shall disclose responsive data by sending it to the Federal Bureau of Investigation at 7747 Clyo Road, Centerville, Ohio, 45459, or making the data available to the Federal Bureau of Investigation via the Provider's electronic portal.

II. Information to be seized by the government

Items evidencing violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography) and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) and 2252A(a)(5)(B) and (b)(1) (possession of child pornography) from September 5, 2021 to the present, including but not limited to the following:

1. Any visual depictions and records related to the possession, receipt and distribution of child pornography.

2. Any images or videos depicting child pornography.

3. Any and all child erotica, including images and videos of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.

4. Any Internet or search history indicative of searching for child pornography or content involving children.

5. Any communications with others in which child exploitation materials and offenses are discussed and/or traded.

6. Any communications with minors, and any identifying information for these minors.

7. Any information related to the use of aliases.

8. Evidence of utilization of email accounts, social media accounts, online chat programs, and peer-to-peer file sharing programs.

9. Evidence of utilization of telephone accounts, Internet Service Providers, and other Electronic Service Providers, including but not limited to monthly statements.

10. Any information related to Internet Protocol (IP) addresses accounts accessed by the accounts.

11. Any geo-location information for the account or other records reflective of the whereabouts of the account user.

12. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

ATTACHMENT C-1

Code Section	Offense Description
18 U.S.C. §2252(a)(4)(B) & (b)(2)	Possession of Child Pornography
18 U.S.C. §2252A(a)(5)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §2252(a)(2) & (b)(1)	Receipt and Distribution of Child Pornography
18 U.S.C. §2252A(a)(2) & (b)(1)	Receipt and Distribution of Child Pornography

ATTACHMENT A-2

Information associated with the Kik account with the user name of **Sentai_Sensei** and the Kik group account with the group name of **#underfifteen** that is stored at premises controlled by MediaLab.ai Inc., a company that accepts service of legal process at 1237 7th Street, Santa Monica, California, 90401.

ATTACHMENT B-2
Particular Things to be Seized

I. Information to be disclosed by MediaLab.ai Inc. (the "Provider")

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, including any e-mails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-2 for the time period of September 12, 2021 through the present:

For the User Account Listed in Attachment A-2:

1. Basic subscriber data, including the current first and last name and email address, link to the most current profile picture or background photograph, device related information, account creation date and Kik version, birthday and email address used to register the account, and user's location information (including IP addresses).
2. Transactional chat logs: logs of all the messages that the user has sent and received, including senders' usernames, receiver usernames / receiver group JID's, timestamps, IP addresses of the senders, and word counts;
3. Chat platform logs: logs of all the media files that the user has sent and received, including senders' usernames, receivers' usernames / receiver JID's, timestamps, IP addresses of the senders, media type, and Content ID's;
4. Photographs and/or videos sent or received by the user for the last 30 days;
5. Roster logs: logs of usernames added and blocked by the user (including timestamps);
6. Abuse reports: transcripts of reported chat histories against the user, including the sender usernames, receiver usernames, timestamps, actual messages, and content ID's;
7. Email events: logs of all the emails that have been associated with the user; and
8. Registration IP's: IP addresses associated to the user when the account was registered (including the timestamps).

For the Group Account Listed in Attachment A-2:

9. Group information logs, including the group JID, group name(s), group type, and the status of the group;
10. Group create logs, including details about who created the group and at what time;
11. Group join logs, including timestamps and the method that was used to join a group;
12. Group leave logs, including timestamps and the method that was used to leave the group;

13. Group transactional chat logs, including sender username, timestamps, IP of the sender, receiver username(s), and word count;
14. Group chat platform logs, including sender username, timestamps, IPs of the sender, receiver username(s), media type, and content ID;
15. Photographs and/or videos received by the group;
16. Group abuse reports, including sender username, receiver username, timestamps, actual message, and content ID's.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant. Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, the Provider shall disclose responsive data by sending it to the Federal Bureau of Investigation at 7747 Clyo Road, Centerville, Ohio, 45459, or making the data available to the Federal Bureau of Investigation via the Provider's electronic portal.

II. Information to be seized by the government

Items evidencing violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography) and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) and 2252A(a)(5)(B) and (b)(1) (possession of child pornography) from September 12, 2021 to the present, including but not limited to the following:

1. Any visual depictions and records related to the possession, receipt and distribution of child pornography.

2. Any images or videos depicting child pornography.

3. Any and all child erotica, including images and videos of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.

4. Any communications with others in which child exploitation materials and offenses are discussed and/or traded.

5. Any communications with minors, and any identifying information for these minors.

6. Any information related to the use of aliases.

7. Evidence of utilization of email accounts, social media accounts, online chat programs, and peer-to-peer file sharing programs.

8. Evidence of utilization of telephone accounts, Internet Service Providers, and other Electronic Service Providers, including but not limited to monthly statements.

9. Any information related to Internet Protocol (IP) addresses accounts accessed by the accounts.

10. Any geo-location information for the account or other records reflective of the whereabouts of the account user.

11. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

ATTACHMENT C-2

Code Section	Offense Description
18 U.S.C. §§ 2252(a)(4)(B) & (b)(2)	Possession of Child Pornography
18 U.S.C. §§ 2252A(a)(5)(B) & (b)(2)	Possession of Child Pornography
18 U.S.C. §§ 2252(a)(2) & (b)(1)	Receipt and Distribution of Child Pornography
18 U.S.C. §§ 2252A(a)(2) & (b)(1)	Receipt and Distribution of Child Pornography